WHAT IS CLAIMED IS:

1. The use of an optical disc, commonly referred to as "Compact Disc" or Digital Versatile Disc" that contains an embedded and encrypted digital signature for the use of signing legal and financial transactions over a networked environment or over the Internet.

2. The storage of a digital signature or digital certificate on a CD-ROM, CD-R, CD-RW or DVD disc for purpose of making the digital signature portable for use on several different computers without expert knowledge in the field of digital certificates.

3. The storage of a digital signature on a compact or DVD disc in encrypted form for the reasons of providing security.

4. The use of more than one digital signature on a single disc for the purpose of providing new digital signatures on a rotating or annual basis.

5. The use of more than one digital signature on a single disc for the purpose of providing immediately available additional digital signatures in the event that the current digital signature is compromised and can no longer be used in a secure manner.

6. The method of incorporating the date as part of the encryption key for protecting the digital signature. The date is added as a portion of the password or pass phrase to form a new password. The new unique password or pass phrase is then used to decrypt a new digital signature. The date can appear as either some numeric form of the date or as an obscured pass phrase or worded term.

7. The use of a software module to decrypt the digital signature contained on a compact disc or other form of media in a manner such that secure data to access the digital signature is entered and processed locally without allowing the entered password or pass phrase to leave the local computer memory.

8. The use of downloadable software components for the purpose of decrypting the digital signature. The source of the software components may be provided locally by residing on the disc containing the digital signature, as part of a third party software package or provided from a remote computer via a network environment.

9. The use of downloadable software components for the specific purpose of aging the digital signature or certificate with or without the user's knowledge. Such components would seek out the next available digital signature or certificate on an automatic basis.

10. The use of the password or pass phrase to provide the key for encrypting the digital signature thus ensuring that the actual digital signature is never entered as data to the local computer.

11. The use of multiple passwords or personal identification number values to determine which of the multiple digital signatures will be accessed.

12. The presentation of a scanned digital image of the user's signature as representation that the digital signature has been accessed properly and has been placed on the electronic document.

13. The use of providing a public key along with the document to ensure the public key is never lost and to provide easy access to the public key. The public key must be used to verify the authenticity of a document that was guarded through the use of a private key.

14. The recording of the digital signature data block a multitude of times on the storage media to provide recovery in the event that one or more images of the digital signature cannot be read from the media.

15. The use of the invention to identify to a high degree the owner of the invention for the purpose of cashing payroll or personal checks over the Internet.

16. The use of the invention for the purpose of identifying the user for certified mail concepts involving electronic mail.

17. The use of the invention to allow the printing of transferred checks that are delivered over the Internet.

18. The use of the invention as a form of identification for the purpose of conducting income tax transactions and receiving and printing refund checks or transferring the refund monies from one account to another.

19. The use of the invention as a key to access personal computers. The key is created by placing the invention into the CD or DVD drive normally found on portable computers and allowing the computer's BIOS or startup code to access the invention to ensure the proper user prior to allowing the rest of the operating system to be loaded.

20. The use of the invention as a key to access computers that are being delivered from the manufacturer to the buyer. The invention is shipped separately, such as by U.S. Mail, while the computer is sent by truck or air. Should the computer become lost or stolen, it is

useless without the invention to start it up. This in turn would make the attempts to steal or hijack such shipments less desirable to thieves.